Yee & Associates, P.C.

4100 Alpha Road
Suite 1100
Dallas, Texas 75244

Main No. (972) 385-8777
Facsimile (972) 385-7766

Facsimile Cover Sheet

To: Commissioner for Patents for **Examiner Aaron C. Perez-Daple** **Group Art Unit 2154**	Facsimile No.: **703/872-9306**
From: Carrie Parker Legal Assistant to Wayne P. Bailey	No. of Pages Including Cover Sheet: **28**

Message:

Enclosed herewith:

- Transmittal Document; and
- Appeal Brief.

Re: Application No. **09/755,351**
Attorney Docket No: **RSW920000175US1**

Date: Tuesday, February 01, 2005

Please contact us at (972) 385-8777 if you do not receive all pages indicated above or experience any difficulty in receiving this facsimile.

PLEASE CONFIRM RECEIPT OF THIS TRANSMISSION BY FAXING A CONFIRMATION TO 972-385-7766.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Cuomo et al.**

Serial No.: **09/755,351**

Filed: **January 5, 2001**

For: **Method and Apparatus for Processing Requests in a Network Data Processing System Based on a Trust Association Between Servers**

§
§
§
§
§
§
§

Group Art Unit: **2154**

Examiner: **Perez-Daple, Aaron C.**

Attorney Docket No.: **RSW920000175US1**

36736
PATENT TRADEMARK OFFICE
CUSTOMER NUMBER

Certificate of Transmission Under 37 C.F.R. § 1.8(a)
I hereby certify this correspondence is being transmitted via facsimile to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, facsimile number (703) 872-9306 on February 1, 2005.

By: Carrie Parker
Carrie Parker

TRANSMITTAL DOCUMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:
ENCLOSED HEREWITH:

- Appeal Brief (37 C.F.R. 41.37).

A fee of $500.00 is required for filing an Appeal Brief. Please charge this fee to IBM Corporation Deposit Account No. 09-0461. No additional fees are believed to be necessary. If, however, any additional fees are required, I authorize the Commissioner to charge these fees which may be required to IBM Corporation Deposit Account No. 09-0461. No extension of time is believed to be necessary. If, however, an extension of time is required, the extension is requested, and I authorize the Commissioner to charge any fees for this extension to IBM Corporation Deposit Account No. 09-0461.

Respectfully submitted,

Duke W. Yee
Registration No. 34,285
YEE & ASSOCIATES, P.C.
P.O. Box 802333
Dallas, Texas 75380
(972) 385-8777
ATTORNEY FOR APPLICANTS

PATENT

Docket No. RSW920000175US1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Cuomo et al.**

Serial No. **09/755,351**

Filed: **January 5, 2001**

For: **Method and Apparatus for Processing Requests in a Network Data Processing System Based on a Trust Association Between Servers**

Group Art Unit: **2154**

Examiner: **Perez-Daple, Aaron C.**

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Certificate of Transmission Under 37 C.F.R. § 1.8(a)
I hereby certify this correspondence is being transmitted via facsimile to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, facsimile number (703) 872-9306 on February 1, 2005.

By: Carrie Parker
Carrie Parker

APPEAL BRIEF (37 C.F.R. 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on December 1, 2004.

The fees required under § 41.20(B)(2), and any required petition for extension of time for filing this brief and fees therefore, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

REAL PARTY IN INTEREST

The real party in interest in this appeal is the following party: International Business Machines Corporation.

RELATED APPEALS AND INTERFERENCES

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no such appeals or interferences.

STATUS OF CLAIMS

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-37

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims canceled: 6-9, 13-17, 24-28, 34 and 36
2. Claims withdrawn from consideration but not canceled:
3. Claims pending: 1-5, 10-12, 18-23, 29-33, 35 and 37
4. Claims allowed: none
5. Claims rejected: 1-5, 10-12, 18-23, 29-33, 35 and 37

C. CLAIMS ON APPEAL

The claims on appeal are: 1-5, 10-12, 18-23, 29-33, 35 and 37

STATUS OF AMENDMENTS

No amendment after final was filed for the present application.

SUMMARY OF CLAIMED SUBJECT MATTER

A. CLAIM 1 - INDEPENDENT

Claim 1 is directed to a method for authenticating a request in a data processing system. The method comprises steps of (1) receiving, by a first security server, a request from a client (Specification page 14, lines 12-16; Figure 3, 'servlet request' to server 302; Figure 5, block 500), (2) performing authentication of the request by the first security server (Specification page 14, lines 16-25; Figure 5, block 502), (3) adding, by the first security server, information to the request to form a modified request, wherein the information indicates that the request is from a trusted source (Specification page 14, lines 26-28; Figure 5, block 506), (4) sending, by the first security server, the modified request to a web application server (Specification page 14, line 28 – page 15, line 7; Figure 5, block 508), (5) presenting the modified request to each of a plurality of components of the web application server, where each of the plurality of components correspond with one of a plurality of security servers (Specification page 19, line 26 – page 20, line 7; Figure 6), and (6) validating, by a one of the plurality of components that corresponds with the first security server, the modified request (Specification page 20, line 8 –page 21, line 23; Figure 6).

B. CLAIM 18 - INDEPENDENT

Claim 18 is directed to a data processing system. The data processing system (Figure 3, element 304) comprises a bus system, a communications unit connected to the bus system, a memory connected to the bus system, wherein the memory includes a plurality of components as a set of instructions, and a processing unit connected to the bus system. The processing unit, responsive to receiving a modified request (Figure 3, 'servlet request') from a first security server (Figure 3, element 302) of a plurality of security servers, executes the set of instructions and presents the request to each of a plurality of components (Figure 3, elements 312, 314 and 316) of the data processing system, wherein each of the plurality of components corresponds with a respective one of the plurality of security servers. The processing unit, responsive to execution of a one of the plurality of components that corresponds with the first security server, determines whether an expected value of information added to the modified request by the first security server is present in the request and processes the request in response to the expected value being present in the

request (Specification page 14, line 9 – page 17, line 10; page 19, line 17 – page 21, line 23; Figure 6).

C. CLAIM 19 - INDEPENDENT

Claim 19 is directed to a network data processing system. Such network data processing system comprises a network (Figure 1, element 102, a plurality of clients connected to the network (Figure 1, elements 108, 110, 112), a first security server connected to the network (Figure 1, element 104), where the first security server receives a request from a client to access a resource (Specification page 14, lines 12-16; Figure 3, 'servlet request' to server 302; Figure 5, block 500), performs an authentication process with the client (Specification page 14, lines 16-25; Figure 5, block 502), adds information to the request in which the information indicates that the request is from a trusted source to form a modified request (Specification page 14, lines 26-28; Figure 5, block 506), and sends the modified request for processing (Specification page 14, line 28 – page 15, line 7; Figure 5, block 508). This network data processing system also comprises a second server connected to the network (Figure 1, element 114), where the second server receives the modified request from the first security server (Specification page 19, lines 26-27; Figure 6, block 600), presents the modified request to a plurality of components each respectively corresponding to a one of a plurality of security servers (Specification page 19, line 27 – page 20, line 7; Figure 6), determines whether the first server is a trusted server based on a determination made by a first component of the plurality of components that corresponds with the first security server (Specification page 20, lines 8-25; Figure 6), and provides access to the resource in response to a determination that the first server is a trusted server (Specification page 20, line 25 – page 21, line 23; Figure 6).

D. CLAIM 29 - INDEPENDENT

Claim 29 is directed to a data processing system for processing a request. This data processing system comprises (1) receiving means for receiving a modified request from a first security server of a plurality of security servers, where the modified request is generated from a request originated by a client and the modified request includes information added by the first security server (Specification page 19, lines 26 – 27; equivalent structure shown at Figure 3, element 304), (2) a plurality of determining means each for determining whether the information present

in the request has an expected value, wherein each of the plurality of determining means corresponds to one of the plurality of security servers (Specification page 19, line 27 – page 20, line 20; equivalent structure shown at Figure 3, element 304 including elements 312, 314 and 316), and (3) processing means for processing the request in response to a one of the plurality of determining means determining the information has the expected value (Specification page 20, line 25 – page 21, line 23; equivalent structure shown at Figure 3, element 304).

E. CLAIM 37 - INDEPENDENT

Claim 37 is directed to a computer program product in a computer readable medium for performing the functions recited in Claim 29.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. GROUND OF REJECTION 1 (Claims 1-5, 10-12, 18-23, 29-33, 35 and 37)

Claims 1-5, 10-12, 18-23, 29-33, 35 and 37 stand rejected under 35 U.S.C. § 103 as unpatentable over Abdelnur et al. (US 6,212,640 B1) in view of Lee et al. (US 6,167,522).

ARGUMENT

A. GROUND OF REJECTION 1 (Claims 1-5, 10-12, 18-23, 29-33, 35 and 37)

A.1. Claim 1

Appellants urge that to establish prima facie obviousness of a claimed invention, all of the claim limitations must be taught or suggested by the prior art. MPEP 2143.03. *See also, In re Royka*, 490 F.2d 580 (C.C.P.A. 1974). In this particular case, all of the claim limitations are not taught or suggested by the cited references. For example, amended claim 1 recites the following:

> 1. A method in a data processing system for authenticating a request, the method comprising:
> receiving, by a first security server of a plurality of security servers, a request from a client;
> performing authentication of the request by the first security server;
> adding, by the first security server, information to the request to form a modified request, wherein the information indicates that the request is from a trusted source;
> sending, by the first security server, the modified request to a web application server;
> presenting the modified request to each of a plurality of components of the web application server, wherein each of the plurality of components correspond with a respective one of the plurality of security servers; and
> validating, by a one of the plurality of components that corresponds with the first security server, the modified request.

As described in the present application and as claimed by claim 1, a plurality of trust association interceptors implemented as components within a web application server are presented with the modified request. Each component corresponds with a respective one of a plurality of security servers (See, e.g., Page 15, Lines 23-27; Page 17, Lines 7-10 and Lines 23-24; and Page 18, Lines 4-7; and Page 19, Lines 27-28). One of the plurality of components validates the modified request (Page 15, Line 27-Page 16, Line 1), for example by requiring a user name representing the proxy server to be included in the modified request. Thus, a one of the plurality of components validates trust with the security server that received and modified the request from the client. For example, Figure 3 shows the following:

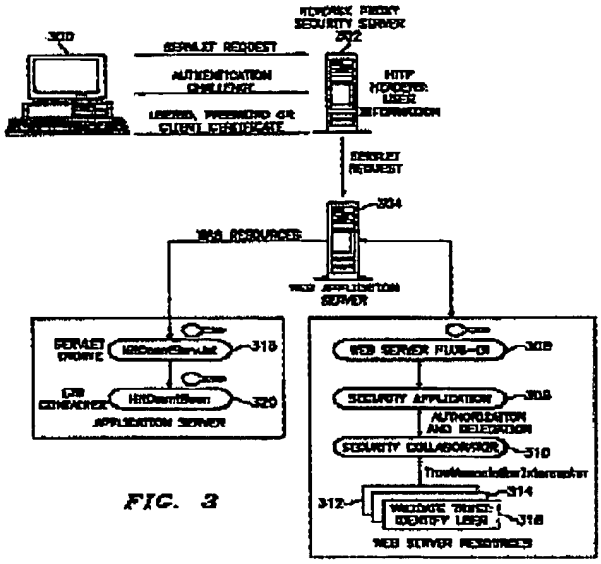

FIG. 3

As can be seen, a web server application includes a plurality of components (trust association interceptors 312, 314, and 316) that, together with a security collaborator of the web application server, receive a request from the web application server that has been modified by a security server (reverse proxy security server 302). Each component (interceptor) corresponds to one of a plurality of security servers and facilitates trust validation with the corresponding security server. The set of components thereby facilitates trust validation among a set of security servers for supporting different security restrictions to a resource.

Abdelnur neither teaches or suggests a method that facilitates a backend server, e.g., a web application server, to support multiple reverse proxy security servers that may feature different security restrictions. Particularly, Abdelnur neither teaches or suggests a system or method having a "plurality of components" that each "correspond with a respective one of" a "plurality of security servers." Thus, Abdelnur fails to teach or suggest a system or method for validating "by a one of the plurality of components that corresponds with the" security server that received a request from a client.

The Examiner expressly acknowledges this deficiency in the Abdelnur teachings, but states that the cited Lee reference teaches this claimed feature of a plurality components that each correspond with a respective one of a plurality of security servers at Lee column 3, lines 9-50. Appellants urge that there, Lee states:

> An application program that is to be provided by a Web server along with a source identifier is received by the Web server via a network, such as, the Internet. The source identifier functions as an indication of sponsorship. The entity sponsoring, or vouching for, the reliability of the application program signs the application program. Thus, the level of trust afforded the signing entity is granted to applications programs signed by that entity.
>
> Before loading the application program, the server performs a verification procedure including granting access privileges based on the source identifier. Access privileges are granted or withheld for resources available to the server. If an application program is received from a known hostile source, or if no access privileges are granted, the applications program may be rejected. Thus, the resources defining the application program's universe, or sandbox, are determined individually based on source identifiers.

As can be seen, this passage describes a technique for a server to verify a received application program (received from a third party who desires that the server distribute such application program to others, per Lee column 2, lines 25-31), including granting access privileges based on the source identifier of where the received application program came from. Notably, this passage does not teach or otherwise suggest sending, by the first security server, the modified request to a web application server; presenting the modified request *to each of a plurality of components of the web application server, wherein each of the plurality of components correspond with a respective one of the plurality of security servers*; and validating, by a one of the plurality of components that corresponds with the first security server, the modified request. Rather, this cited passage teaches that (1) a single server validates (2) an application program. There is no teaching or suggestion, in this cited Lee passage, of (i) a modified request, or (ii) the presenting of such (non-existent) modified request *to each of a plurality of components of the web application server*, wherein each of the plurality of components correspond with a respective one of the plurality of security servers.

Still further with respect to Claim 1, Applicants urge that none of the cited references teach or suggest steps of (1) performing authentication of the request by the first security server, and (2) adding, by the first security server, information to the request to form a modified request, wherein the information indicates that the request is from a trusted source. In rejecting this aspect of Claim 1, the Examiner alleges that Abdelnur teaches these two steps by the operation of web server 480 as described at Abdelnur at col. 11, line 47 – col. 12, line 6 and as shown in Figures 4 and Figure 6 (block 610). Applicants urge two-fold error in this assertion. First, the web server 480 performs an

authorization check (col. 11, lines 43-52), and does not perform an *authentication* process with a client – authorization and authentication being very different things (as per Abdelnur column 11, lines 45-52, an authorization check is made to determine whether the application is *authorized to access a resource*). Claim 1 expressly recites performing authentication of a request, which is different from performing resource authorization as described by Abdelnur (see also the present Specification at page 16, lines 12-14 and page 21, lines 6-23 where authentication and authorization are described to be different actions). Secondly, Abdelnur's web server 480 does not add any information to the request that indicates that the request is from a trusted source. Rather, the request is merely converted to a proper format before being forwarded to server 460 (Abdelnur col. 11, lines 57-60). Thus, there are additional claimed steps not taught or suggested by the cited references.

Therefore, as all of the claim limitations are not taught or suggested by the cited references, it is shown that a prima facie case of obviousness has not been established by the Examiner. Accordingly, the rejection of Claim 1 is improper and should be overturned[1].

A.2. Claim 18 (and Claim 11)

Applicants urge that none of the cited references teach or suggest the claimed feature of a processing unit, responsive to receiving a modified request from a first security server of a plurality of security servers, executes the set of instructions and presents the request *to each of a plurality of components of the data processing system, wherein each of the plurality of components corresponds with a respective one of the plurality of security servers*, and wherein the processing unit, responsive to execution of a one of the plurality of components that corresponds with the first security server, *determines whether an expected value of information added to the modified request by the first security server is present in the request and processes the request in response to the expected value being present in the request.* This process is described in the preferred embodiment at Specification page 20, line 25 – page 21, line 23 as pertaining to user authentication. In rejecting Claim 18, the Examiner relies upon the same

[1] If the examiner fails to establish a prima facie case, the rejection is improper and will be overturned. *In re Fine*, 837 F.2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988)

reasoning as given in the rejection of Claim 1 regarding a determination of whether a server is a trusted server. The scope of Claim 18 is different from that of Claim 1, in that Claim 18 expressly recites a determination of whether an expected value of information added to the modified request by the first security server is present in the request and processes the request in response to the expected value being present in the request. The cited Lee passage purporting to teach this claimed feature does not teach a conditional action (process the request) *in response to* expected value added to the modified request being present in such request. Rather, the cited Lee reference teaches granting or denying access privileges for a received application program based on a source identifier. This Lee source identifier is always there, so there is no conditional operation that is performed based upon whether such source identifier was added or not. Rather, the (always present) source identifier is used in the determination of whether or not to grant or deny access privileges by the application program that was received with the source identifier (Lee Col. 3, lines 9-50). In addition, this has nothing to do with user authentication, which is accomplished in the preferred embodiment using the techniques recited in Claim 18. Thus, Claim 18 is shown to have been erroneously rejected as all claim limitations are not taught or suggested by the cited references.

With respect to Claim 11, and in addition to reasons given above with respect to independent Claim 1 (of which Claim 11 depends upon), Applicants urge that none of the cited references teach or suggest *a validation that is conditional upon an expected value being in a data structure*, for similar reasons to those described above with respect to Claim 18 and the user authentication process. Thus, Claim 11 is further shown to have been erroneously rejected as all claim limitations are not taught or suggested by the cited references.

A.3. Claim 19

With respect to Claim 19, Applicants urge that none of the cited references teach or suggest a first security server that both (1) performs an authentication process with a client (from which it receives a resource access request), and (2) adds information to such request in which the information indicates that the request is from a trusted source. In rejecting Claim 19, the Examiner states that Abdelnur teaches these two steps by the operation of web server 480 as described at Abdelnur at col. 11, line 47 – col. 12, line 6 and as shown in Figures 4 and Figure 6 (block 610). Applicants urge two-fold error in this assertion. First, the web server 480 performs an

authorization check (col. 11, lines 43-52), and does not perform an *authentication* process with a client – authorization and authentication being very different things (as per Abdelnur column 11, lines 45-52, an authorization check is made to determine whether the application is *authorized to access a resource*). Claim 19 expressly recites performing an authentication process, which is different from performing resource authorization as described by Abdelnur (see also the present Specification at page 16, lines 12-14 and page 21, lines 6-23 where authentication and authorization are described to be different actions). Secondly, Abdelnur's web server 480 does not add any information to the request that indicates that the request is from a trusted source. Rather, the request is merely converted to a proper format before being forwarded to server 460 (Abdelnur col. 11, lines 57-60). Thus, as the Examiner's rationale in rejecting Claim 19 is shown to be in error, it is urged that a prima facie case of obviousness has not been established with respect to Claim 19, as all claimed elements are not taught or suggested by the cited references.

Still further with respect to Claim 19, Applicants urge that none of the cited references teach or suggest the claimed "plurality of components each respectively corresponding to a one of a plurality of security servers" for similar reasons to those described above with respect to Claims 1 and 18.

A.4. Claim 20

Claim 20 is a further refinement of Claim 19 be introducing specific operational characteristics of a second security server, which is in addition to the claimed first security server. In rejecting Claim 20, the Examiner states that the cited Lee reference teaches providing a second security server performing the same functions as the first security server, wherein the second security server contains a second component corresponding to the second security server for determining different security restrictions for the second security server at Fig. 1 and column 3, lines 9-50. Applicants show error in such assertion. Lee teaches but a single web server (Figure 1, element 150). The hosts shown in Figure 1 at 120, 122, 124 and 126 do not perform any type of client authentication or determination of a trusted server, both of which are expressly recited in Claim 20 as being performed by the claimed second security server. Rather, Lee's hosts 120, 122, 124 and 126 provide applications to web server 150, for subsequent distribution (Lee column 3, lines 34-35). While Lee states that hosts 120, 122, 124 and 126 may also act as Web servers to provide files or resources to other hosts (column 3, lines 26-30), there is no teaching or suggest that

as a part of providing files or resources to other hosts, these hosts 120, 122, 124 and 126 (i) perform an authentication process with clients, (ii) add information to a request received from a client indicating that the requests are from a trusted source, or (iii) that different security restrictions are provided by the first component and the second component. Thus, Claim 20 is further shown to have been erroneously rejected as there are numerous claimed features not taught or suggested by the cited references.

A.5. Claims 29 and 37

With respect to Claim 29 (and similarly for Claim 37), Appellants urge that none of the cited references teach or suggest "a plurality of determining means each for determining whether the information present in the request has an expected value, wherein each of the plurality of determining means corresponds to one of the plurality of security servers". As can be seen, there are several aspects to this claimed feature. First, there are a plurality of determining means each for determining something. Second, each of these plurality of determining means corresponds to one of the plurality of security servers. Third, the determining means determines whether the information present in the request has an expected value. Applicants urge that none of the cited references teach or suggest any of these three aspects of Claim 29. Contrary to the Examiner's assertion with respect to the cited Lee reference, Lee does not teach/suggest a plurality of components in a server for determining information in a (received) request, and Lee does not teach/suggest that each of these plurality of components corresponds to one of a plurality of security servers. These aspects of Claim 29 have previously been discussed above with respect to Claim 1. Finally, none of the cited references teach/suggest that these (missing) plurality of determining means determines whether information present in the request has an expected value. This aspect of Claim 29 has previously been discussed above with respect to Claim 18. Thus, Claims 29 and 37 are shown to have been erroneously rejected as there are numerous claimed features not taught or suggested by the cited references.

A.6. Claim 32

With respect to Claim 32, Applicants urge that none of the cited references teach or suggest the claimed feature of "wherein the information is an identification of the first security server". This claimed feature advantageously provides an ability to signal the back-end server that a

particular security server, as per the first security server identification, authenticated the request (Specification page 18, lines 3-11). In rejecting Claim 32, the Examiner states that this claimed feature is taught by Abdelnur at col. 9, lines 60-64 (this identical passage is also cited when rejecting Claim 33, which instead of reciting that the information is an identification of the first security server, Claim 33 recites that the information is an identification of a user of the client). Appellants urge that this cited Abdelnur passage mentions use of a user name and password pertaining to a client application, but docs not teach or suggest that *information added by a security server is an identification of such security server*. Thus, it is shown that Claim 32 has been erroneously rejected as there are claimed features not taught or suggested by any of the cited references.

A.7. Claim 35

With respect to Claim 35, Applicants urge that none of the cited references teach or suggest the claimed feature of "wherein the plurality of determining means includes a set of interceptors that can provide different security restrictions to a resource". As can be seen, different security restrictions for a given resource are provided by the set of interceptors, thus advantageously supporting a plurality of different security restrictions which enables operation of a given back-end server with a plurality of different types of front-cnd security servers (Specification page 20, lines 8-13). In rejecting Claim 35, the Examiner states that interceptors are inherent. Applicants urge that Claim 35 goes beyond a mere recitation of interceptors, and Claim 35 specifically states a particular function performed by such interceptors. Even assuming arguendo that interceptors are inherent, such allegation does not establish a teaching, suggestion, or inherency regarding providing different security restrictions to a resource by such (alleged inherent) interceptors. Thus, the Examiner has failed to establish a prima facie showing of obviousness with respect to Claim 35, and therefore Claim 35 is shown to have been erroneously rejected.

In conclusion, Appellants have shown numerous instances of error in the rejection of Claims 1-5, 10-12, 18-23, 29-33, 35 and 37 under 35 U.S.C. 103, and accordingly requests that the rejection of such claims be reversed by the Board.

Duke W. Yee
Reg. No. 34,285
Wayne P. Bailey
Reg. No. 34,289
YEE & ASSOCIATES, P.C.
PO Box 802333
Dallas, TX 75380
(972) 385-8777

CLAIMS APPENDIX

The text of the claims involved in the appeal are:

1. A method in a data processing system for authenticating a request, the method comprising:

receiving, by a first security server, a request from a client;

performing authentication of the request by the first security server;

adding, by the first security server, information to the request to form a modified request, wherein the information indicates that the request is from a trusted source;

sending, by the first security server, the modified request to a web application server;

presenting the modified request to each of a plurality of components of the web application server, wherein each of the plurality of components correspond with a respective one of a plurality of security servers; and

validating, by a one of the plurality of components that corresponds with the first security server, the modified request.

2. The method of claim 1, wherein the request is a request to access data.

3. The method of claim 1, wherein the first security server is a reverse proxy server.

4. The method of claim 1, wherein the information includes a user identification.

5. The method of claim 1, wherein the information includes an identification of the first security server.

10. The method of claim 4, wherein the user identification is a user name and password.

11. The method of claim 1, wherein the step of validating further comprises determining that a value of the information is an expected value located in a data structure.

12. The method of claim 1, wherein each of the plurality of components is implemented as a respective interceptor.

18. A data processing system comprising:

a bus system;

a communications unit connected to the bus system;

a memory connected to the bus system, wherein the memory includes a plurality of components as a set of instructions; and

a processing unit connected to the bus system, wherein the processing unit, responsive to receiving a modified request from a first security server of a plurality of security servers, executes the set of instructions and presents the request to each of a plurality of components of the data processing system, wherein each of the plurality of components corresponds with a respective one of the plurality of security servers, and wherein the processing unit, responsive to execution of a one of the plurality of components that corresponds with the first security server, determines whether an expected value of information added to the modified request by the first

security server is present in the request and processes the request in response to the expected value being present in the request.

19. A network data processing system comprising:

a network;

a plurality of clients connected to the network;

a first security server connected to the network, wherein the first security server receives a request from a client to access a resource, performs an authentication process with the client, adds information to the request in which the information indicates that the request is from a trusted source to form a modified request, and sends the modified request for processing; and

a second server connected to the network, wherein the second server receives the modified request from the first security server, presents the modified request to a plurality of components each respectively corresponding to a one of a plurality of security servers, determines whether the first server is a trusted server based on a determination made by a first component of the plurality of components that corresponds with the first security server, and provides access to the resource in response to a determination that the first server is a trusted server.

20. The network data processing system of claim 19 further comprising a second security server connected to the network, wherein the second security server receives requests from clients to access the resource, performs an authentication process with the clients, adds information to the requests in which the information indicates that the requests are from a trusted source to form modified requests, and sends the modified requests to the second server for

processing, wherein the second server presents the modified requests of the second security server to each of the plurality of components and determines whether the second security sever is a trusted server based on a determination made by a second component that corresponds with the second security server, wherein the first component and the second component provide different security restrictions.

21. The network data processing system of claim 19, wherein the network is at least one of a local area network, an intranet, an extranet and an Internet.

22. The network data processing system of claim 19, wherein the plurality of components comprise a set of interceptors in which the set of interceptors are used to determine whether the first security server is a trusted server, wherein the request is sent to each of the set of interceptors to determine whether the interceptors can handle the request.

23. The network data processing system of claim 19, wherein the second server receives the request directly from the client.

29. A data processing system for processing a request, the data processing system comprising:

receiving means for receiving a modified request from a first security server of a plurality of security servers, wherein the modified request is generated from a request originated by a client and the modified request includes information added by the first security server;

a plurality of determining means each for determining whether the information present in

the request has an expected value, wherein each of the plurality of determining means corresponds to one of the plurality of security servers; and

processing means for processing the request in response to a one of the plurality of determining means determining the information has the expected value.

30. The data processing system of claim 29, wherein the modified request requests access to a resource, the data processing system further comprising:

second determining means for determining whether a user of the client is authorized to access the resource; and

accessing means for accessing the resource using the modified request in response to a determination that the user is authorized.

31. The data processing system of claim 29, wherein the first security server is a reverse proxy server.

32. The data processing system of claim 29, wherein the information is an identification of the first security server.

33. The data processing system of claim 29, wherein the information is a user name and password of a user of the client.

35. The data processing system of claim 29, wherein the plurality of determining means includes a set of interceptors that can provide different security restrictions to a resource.

37. A computer program product in a computer readable medium for processing a request, the computer program product comprising:

first instructions for receiving a modified request from a first security server, wherein the modified request is generated by the first security server by modifying information in a request originated by a client;

second instructions for determining one of a plurality of interceptors that can process the request;

third instructions for determining whether a value of the information present in the request is an expected value; and

fourth instructions, responsive to the value of the information being the expected value, for processing the request.

EVIDENCE APPENDIX

There is no evidence to be presented.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings.